Encuentran más de 40 aplicaciones con más de 100 millones de instalaciones que fugan claves de AWS

Autor: I. Stepanenko

Fecha: Friday 14th of May 2021 09:47:47 AM

La mayoría de los usuarios de aplicaciones móviles por lo general confían ciegamente en que las aplicaciones que descargan de las tiendas de apps oficiales son seguras y protegidas, pero no siempre es así.

La compañía de ciberseguridad e inteligencia de máquinas, CloudSEK, proporcionó recientemente una plataforma llamada BeVigil donde las personas pueden buscar y verificar las calificaciones de seguridad de las aplicaciones y otros problemas de seguridad antes de instalar una aplicación.

En un último informe, se detalla cómo el motor de búsqueda BeVigil identificó más de 40 aplicaciones, con más de 100 millones de descargas acumuladas, que tenían claves privadas de Amazon Web Services (AWS) codificadas en su interior, *«colocando sus redes internas y sus datos de usuarios en riesgo de ciberataques»*.

Encuentran más de 40 aplicaciones con más de 100 millones de instalaciones que fugan claves de AWS

Autor: I. Stepanenko

Fecha: Friday 14th of May 2021 09:47:47 AM

La fuga de claves de AWS se detectó en algunas de las principales aplicaciones como Adobe Photoshop Fix, Adobe Comp, Hootsuite, IBM´s Weather Channel y los servicios de compras en línea Club Factory y Wholee. Los hallazgos son el resultado de una análisis de más de 10,000 aplicaciones enviadas a BeVigil de CloudSEK, un motor de búsqueda de seguridad de aplicaciones móviles.

> «Las claves de AWS codificadas en el código fuente de una aplicación móvil pueden ser un gran problema, especialmente si su función tiene un alcance y permisos amplios. Las posibilidades de uso indebido son infinitas aquí, ya que los ataques se pueden encadenar y el atacante puede obtener más acceso a toda la infraestructura, incluso la base del código y las configuraciones», dijeron los investigadores de CloudSEK.

CloudSEK dijo que reveló responsablemente las vulnerabilidades de seguridad a AWS y las empresas afectadas de forma independiente.

Organisation	App ID	No. of Installs	Category	Country
Clubfactory	club.fromfactory	100,000,000+	Ecommerce	India
Adobe Photoshopfix	com.adobe.adobephotoshopfix	10,000,000	Photography	United States
Adobe Comp	com.adobe.comp	500,000+	Art & Design	United States
Weather Forecast & Snow Radar	com.weather.weather	100,000,000	Weather	United States
Wholee - Online Shopping Store	com.wholee	1,000,000	Shopping	Singapore
Oven Story Pizza	in.ovenstory	1,000,000	Food & Drink	India
Hootsuite:	com.hootsuite.droid.full	5,000,000	Social	Canada

En una aplicación analizada por la compañía de seguridad cibernética con sede en Bengaluru, la clave de AWS expuesta tenía acceso a múltiples servicios de AWS, incluidas las credenciales para el servicio de almacenamiento S3, que a su vez abrió el acceso a 88 depósitos que contienen 10.073,444 archivos y datos, que ascienden a 5.5 terabytes.

Además, se incluyeron en los depósitos el código fuente, las copias de seguridad de la aplicación, los informes de usuario, los artefactos de prueba, los archivos de configuración y credenciales que podrían usarse para obtener un acceso más profundo a la infraestructura de la aplicación, incluidas las bases de datos de los usuarios.

Las instancias de AWS mal configuradas accesibles desde Internet han sido la causa de muchas violaciones de datos recientemente. En octubre de 2019, la empresa de ciberseguridad Imperva, reveló que la información de un subconjunto no especificado de usuarios de su producto Cloud Firewall, era accesible en línea luego de una migración fallida a la nube de su base de datos de clientes que comenzó en 2017.

El mes pasado, la plataforma de corretaje de descuentos y comercio en línea con sede en India, Upstox, sufrió un incidente de seguridad después de que un notorio grupo de hackers llamado ShinyHunters accediera a su bucket AWS S3 configurado de forma incorrecta.

> «Las claves API codificadas son como cerrar su casa pero dejando la llave en un sobre con la etiqueta 'No abrir'. Estas claves podrían ser descubiertas fácilmente por hackers o competidores malintencionados que podrían usarlas para comprometer sus datos y redes», dijo Shahrukh Ahmad, director de tecnología de BeVigil.

BeVigil es un motor de búsqueda de seguridad móvil que permite a los investigadores buscar metadatos de aplicaciones, revisar su código, ver informes de seguridad y puntuaciones de riesgo e incluso escanear nuevos APK.

Las aplicaciones móviles han sido el objetivo de muchos ataques recientes a la cadena de suministro. Los atacantes inyectan código malicioso en los SDK que utilizan los desarrolladores de aplicaciones. Los equipos de seguridad pueden confiar en BeVigil para identificar cualquier aplicación maliciosa que utilice SDK maliciosos.

Los investigadores de seguridad pueden realizar investigaciones profundas de varias aplicaciones que se encuentran en la web mediante la búsqueda de metadatos. Los informes de escaneo generados por BeVigil están disponibles para toda la comunidad de CloudSEK. En resumen, es similar a VirusTotal para consumidores e investigadores de seguridad.

¿Qué se puede buscar en BeVigil?

Es posible realizar búsquedas en millones de aplicaciones con fragmentos de código vulnerables o palabras clave para saber qué aplicaciones los contienen. Con esto, los investigadores pueden analizar fácilmente datos de calidad, correlacionar amenazas y lidiar con falsos positivos.

Además de buscar una aplicación específica simplemente con el nombre, también se puede encontrar una lista completa de aplicaciones:

De una organización
Por encima o por debajo de una determinada puntuación de seguridad
Lanzado dentro de un período de tiempo determinado
De 48 categorías diferentes como finanzas, educación, herramientas, etc.
De un desarrollador específico mediante la búsqueda con la dirección de correo electrónico del desarrollador
Desarrollador en un país específico mediante la búsqueda
Desarrollado en una ubicación específica mediante la búsqueda con el código pin o la dirección de correo electrónico del desarrollador
Que graban audio de fondo
Ubicación de registro en el fondo
Que puede acceder al dispositivo de la cámara
Que puede acceder a un permiso específico en su dispositivo
Con una versión de SDK de destino específica
Además de estos, también se pueden usar Regexes para encontrar aplicaciones con vulnerabilidades de seguridad buscando patrones de código.